Improvement of CyRIS for Building Various Kinds of Cyber Training Instances

Yuichiro Sakamoto
Tokyo Metropolitan College of Industrial Technology
Tokyo, Japan
m18019@g.metro-cit.ac.jp

Michihiro Kobayakawa
Tokyo Metropolitan College of Industrial Technology
Tokyo, Japan
kobayakawa@acm.org

Ken-ichi Chinen
Japan Advanced Institute of Science and Technology
Ishikawa, Japan
k-chinen@jaist.ac.jp

Razvan Beuran
Japan Advanced Institute of Science and Technology
Ishikawa, Japan
razvan@jaist.ac.jp

***Abstract*—For effective cyber security training, building a virtual training environment corresponding to various cyber training scenarios is essential. However, building a virtual training environment takes time and effort. Thus, a framework for easily building a virtual training environment is indispensable.**

Razvan et al. have proposed a cyber security training framework named CyTrONE. We focus on a cyber range instantiation system called CyRIS and propose an improved CyRIS for building both Linux virtual machines and Windows virtual machines to use for a cyber training instance.

And we confirmed that the improved CyRIS built virtual machines for Linux, Windows 7, Windows 8.1, Windows 10, and Windows Server as instances.

In this paper, we showed that the improved CyRIS could build a virtual training environment corresponding to various cyber training scenarios.

***Index Terms*—Cybersecurity, cyber range, cyber training enviroment.**

I. Introduction

Cyber range is one of the effective systems for developing security skills necessary to respond to various cyberthreat. Some companies such as Boeing, Cisco, IBM, Israel Aerospace Industries, Ixia, Sypris and so on provide a cyber range for cyber security training.

Generally, cyber security training is done in a virtual training environment made by building up a set of virtual machines called an "instance." TABLE I is shown a representative virtual training environment. There are three network segments, 1) DMZ segment, 2) internal server segment, and 3) user client segment. Each computer typically runs either Linux OS or Windows OS.

Razvan et al. have proposed a cyber security training framework named CyTrONE [1]. CyTrONE consists of three systems, 1) training server that provides a description file to LMS and CyRIS, 2) learning management system(LMS), and 3) cyber range instantiation system called CyRIS [2].

This paper focuses on the CyRIS and proposes an improved CyRIS to respond various cyber training scenarios. Our key improvement for CyRIS is to allow us to deploy and setup Windows machines as a virtual training environment.

The rest of paper shows an overview of CyRIS (Section II-A), improvement (Section II-B), an overview of improved CyRIS and confirmations of improved CyRIS (Section III), and conclusion (Section IV).

TABLE I
THE STRUCTURE OF A GENERAL INTRANET

segment	server	OS Type
DMZ	DNS	Windows, Linux
	Web	Windows, Linux
	Mail	Windows, Linux
Internal Server	authentication	Windows, Linux
	file	Windows, Linux
	internal Web	Windows, Linux
	NTP	Windows, Linux
	Proxy	Windows, Linux
	DB	Windows, Linux
User Client	Client machine	Windows

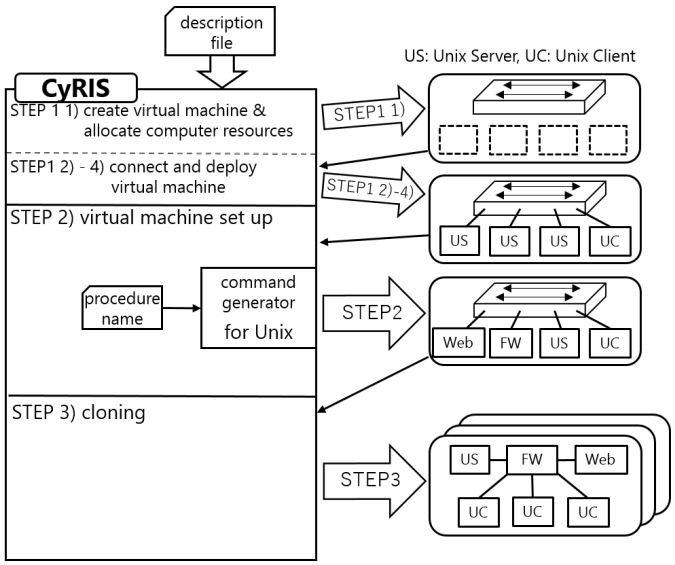

Fig. 1. CyRIS Overview

II. CyRIS

A. Overview

CyRIS is a cyber range instantiation system which works in the CyTrONE. CyRIS receives a description file formatted by YAML and then builds an instance used for a cyber security training. The description file consists of three parts, 1) host_setting, 2) guest_setting, and 3) clone_setting. Fig.2 shows the simplest description file.

```
---
- host_settings:
  - id: host_1
    mgmt_addr: 172.16.1.7
    virbr_addr: 192.168.122.1
    account: cyuser

- guest_settings:
  - id: desktop
    basevm_host: host_1
    basevm_config_file: file_name
    basevm_type: kvm

- clone_settings:
  - range_id: 123
    hosts:
    - host_id: host_1
      instance_number: 1
      guests:
      - guest_id: desktop
        number: 1
        entry_point: yes
      topology:
      - type: custom
        networks:
        - name: office
          members: desktop.eth0
```

Fig. 2. simplist description file

Hereafter, we overview CyRIS. For building virtual machines, CyRIS receives a description file and then executes the following steps:

STEP 1 prepare for deploying and deploy virtual machines
1) assign computer resources to virtual machine and create new virtual machine,
2) connect a virtual machine to a virtual switch,
3) deploy a virtual machine from a base image,
4) start a virtual machine

STEP 2 set up virtual machines
1) set up an IP address,
2) set up SSH connection,
3) manage user accounts,
4) manage application software,

STEP 3 clone virtual machines
1) reconnect networks between virtual machines,
2) clone virtual machines.

In STEP 1, CyRIS deploys a virtual machine from base image by using a hypervisor.

Actually, CyRIS extracts setting parameters from the description file for creating new virtual machines and sends them to the hypervisor.

The hypervisor receives setting parameters from CyRIS and then creates new virtual machine and connect them to virtual switch.

In STEP 2, CyRIS sets up the network of virtual machines and sets each role for each virtual machine. In STEP 3, CyRIS disconnects virtual machines to virtual switch and reconnect the network between virtual machines. The reconnected network is used for cyber security training. We call it an "original instance" for a trainee. For N trainees, CyRIS clones $N-1$ instances from an original instance.

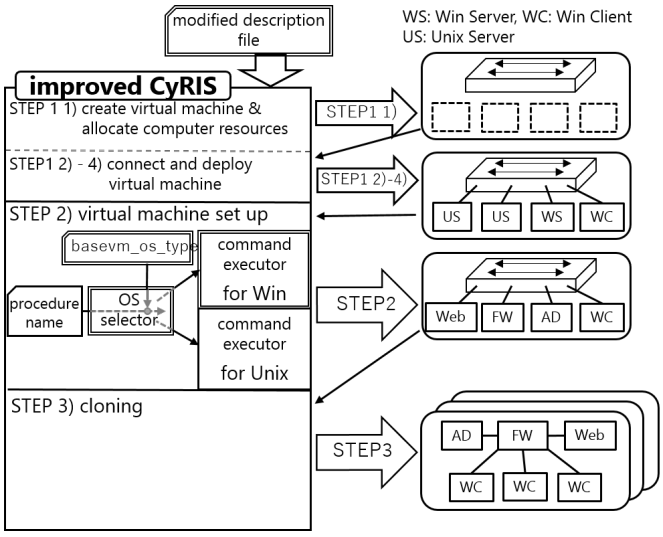

Fig. 3. improved CyRIS Overview

In the original design, CyRIS could set up Linux virtual machines. However, for developing security skills necessary to respond to various cyberthreat, CyRIS is required a variety of virtual training environments. Especially, CyRIS has to be improved to set up virtual machines that run Linux and Windows.

B. Improvement

Improved CyRIS has to allow us to set up various virtual machines that run Linux, Windows 7, Windows 8.1, Windows 10, and/or Windows Server. We have to modify the description file and to improve STEP 2 in CyRIS. Because, there are no descriptions to select os and its version and no mechanism to select them and to set them. Here, we have to improve the procedures（STEP 2) as follows:

1) start a virtual machine
2) select OS type and version,
   a) execute the following procedures corresponding to each OS
      i) set up an IP address,
      ii) set up SSH connection,
      iii) manage user accounts,
      iv) manage application software,

For the description file, we define new keys for setting a virtual machine. The keys defined newly are "number_of_cores", "memory_size", "basevm_os_type". For improving CyRIS, we create new mechanism to select os and its version. The details of the improved CyRIS are shows in the next section.

III. Improved CyRIS

A. Overview of improved CyRIS

We propose an improved CyRIS which allows us to build various virtual machines that run Linux, Windows 7, Windows

TABLE II
DETAILS OF OS USED FOR CONFIRMATION

OS	edition	URL	bit
CentOS 7.3	–	https://github.com/crond-jaist/cyris/releases/download/0.2/basevm_small.tar.gz	64bit
Windows 7	Enterprise	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	32bit
Windows 8.1	nterprise Evaluation	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	64bit
Windows 10	Enterprise 2016 LTSB Evaluation	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise	64bit
Windows Server 2016	Standard Evaluation	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016/	64bit

TABLE III
WHETHER EACH OPERATION COULD BE EXECUTED FOR EACH OS

procedure name	CentOS 7	Windows 7	Windows 8.1	Windows 10	Windows Server
STEP 1 prepare for deploying and deploy virtual machines					
assign computer resources to virtual machine and create new virtual machine	○	○	○	○	○
connect a virtual machine to a virtual switch,	○	○	○	○	○
deploy a virtual machine from a base image	○	○	○	○	○
start a virtual machine	○	○	○	○	○
STEP 2 set up virtual machine					
The virtual mahine sets its own IP address	○	○	○	○	○
set up SSH connection	○	○	○	○	○
manage user accounts	○	○	○	○	○
manage application software	○	○	○	○	○
STEP 3 clone virtual machines					
reconnect networks between virtual machines	○	○	○	○	○
clone virtual machines	○	○	○	○	○

8.1, Windows 10, and/or Windows Server. As similar to the CyRIS, the improved CyRIS receives the modified description file and then builds an instance used for a cyber security training. The procedures for building the virtual training environment of the improved CyRIS are the same as that of the CyRIS. Fig.3 shows an overview of the improved CyRIS.

In this section, we show the procedures of STEP 2 improved to build various types of OSs.

In STEP 2, the improved CyRIS has a function which judges the OS type of a virtual machine and carries out the commands necessary to its OS. We implement a set of script for Windows as follows:

1) script for setting up IP address,
2) script for setting up SSH connection,
3) script for managing user accounts,
4) script for managing application software,

The set of script sets up the original virtual machines to virtual machines for cyber training. From STEP 1 to STEP 3, CyRIS creates instances of each user.

B. Confirmations

We should confirm that improved CyRIS can build a virtual training environment consisting of virtual machines running various OS.

TABLE IV shows the specification of the computer used for confirmations. And we use 1) CentOS 7, 2) Windows 7, 3) Windows 8.1, 4) Windows 10, 5) Windows Server as template images, where file size of a template image and file format for that are 15 GB and qcow2, respectively. TABLE II shows detailed information such as the edition, source URL, and number of these OSs.

TABLE IV
SPECIFICATION OF THE COMPUTER USED FOR CONFIRMATIONS

model number	PowerEdge R430
CPU	Intel ®Xeon ®Processor E5-2603 v4 dual CPUs
memory	128GB
storage	1.9 TB SAS HDD
hypervisor	KVM(Kernel-based Virtual Machine)

We confirmed that improved CyRIS can build virtual training environment consisting of virtual machines running each OS for one trainee.

TABLE III shows the results of confirmations. The first column shows requirements for the improved CyRIS, and each column from the second column to the sixth column shows OS type of virtual machine.

All cells of TABLE 1 have ○, that is, this indicates that the procedures of STEP 1 to STEP 3 of the improved CyRIS were correctly executed.

IV. CONCLUSION

This paper proposed improved CyRIS which allowed us to build various virtual machines that run Linux, Windows 7, Windows 8.1, Windows 10, and/or Windows Server. We confirmed that all procedures from STEP 1 to STEP 3 of the improved CyRIS succeeded in building virtual machines running Linux, Windows 7, Windows 8.1, Windows 10 and/or Windows Server. Our confirmations show that the improved CyRIS can build various cyber training environments corresponding to various cyber training scenarios.

REFERENCES

[1] R. Beuran, C. Pham, D. Tang, K. Chinen, Y. Tan, Y. Shinoda, "CyTrONE: An Integrated Cybersecurity Training Framework, "International Conference on Information Systems Security and Privacy (ICISSP 2017), pp. 157-166, Porto, Portugal, February 19-21, 2017.

[2] C. Pham, D. Tang, K. Chinen, R. Beuran, "CyRIS: A Cyber Range Instantiation System for Facilitating Security Training, "International Symposium on Information and Communication Technology (SoICT 2016), pp. 251-258, Ho Chi Minh, Vietnam, December 8-9, 2016.